NASA/TM—2001-211145

Space Internet-Embedded Web Technologies Demonstration

David A. Foltz
Glenn Research Center, Cleveland, Ohio

National Aeronautics and
Space Administration

Glenn Research Center

September 2001

Trade names or manufacturers' names are used in this report for identification only. This usage does not constitute an official endorsement, either expressed or implied, by the National Aeronautics and Space Administration.

Available from

NASA Center for Aerospace Information
7121 Standard Drive
Hanover, MD 21076

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22100

Available electronically at http://gltrs.grc.nasa.gov/GLTRS

SPACE INTERNET-EMBEDDED WEB TECHNOLOGIES DEMONSTRATION

David A. Foltz
National Aeronautics and Space Administration
Glenn Research Center
Cleveland, Ohio 44135

SUMMARY

The NASA Glenn Research Center recently demonstrated the ability to securely command and control space-based assets by using the Internet and standard Internet Protocols (IP). This is a significant accomplishment because future NASA missions will benefit by using Internet standards-based protocols. The benefits include reduced mission costs and increased mission efficiency. The Internet-Based Space Command and Control System Architecture demonstrated at the NASA Inspection 2000 event proved that this communications architecture is viable for future NASA missions.

INTERNET-BASED SPACE COMMAND AND CONTROL SYSTEM ARCHITECTURE

It seems that just about anywhere you go now you are able to find Internet connectivity close by. Because of this, the Internet has redefined the way we conduct research in today's world. But for the engineers and research scientists at NASA the world is not enough. Several organizations within NASA are working together to extend the Internet beyond the Earth and into space.

Internet Protocols (IP) has established itself as the dominant communications protocol on Earth and the research staff at NASA sees great potential in delivering IP to space. By establishing IP as the protocol of choice for most communications, NASA mission designers can reduce the complexity of the communications systems and save money by using common off-the-shelf devices. This will allow mission designers to incorporate Embedded Web Technologies (EWT) on future payloads which will allow NASA ground controllers and NASA-sponsored researchers direct command and control access of their experiments onboard the spacecraft.

Past NASA missions required the research scientists to travel to a NASA Telescience Support Center to communicate with their experiments onboard a shuttle or space station. This was a large burden to the research community. The best place to control and analyze their onboard experiments was at home where the experiments were created. The new way of thinking is to let the researchers access their data directly from their university or research site. IP onboard the spacecraft is the tool to accomplish this mission.

The ability to operate and retrieve data from a space experiment via the Internet has many positive aspects. The most positive aspect is convenience. Internet connectivity allows the researcher to access the experiment from their research facility. However, there is a price to pay for that convenience. Where there is Internet, there is foul play. The risks are enormous for hacking and cracking penetrations on space-based systems. Before space-based assets are made accessible to the Internet, the security must be rock solid.

On November 1, 2000, the NASA Lyndon B. Johnson Space Center in Houston, Texas, hosted a technology demonstration called Inspection 2000. NASA conducts their annual inspection events to showcase the latest NASA-developed technologies. The Space Operation and Management Office (SOMO) at the Lyndon B. Johnson Space Center has tasked the Glenn Research Center to demonstrate a full working system of a typical NASA mission using Embedded Web Technologies. To properly demonstrate this technology a terrestrial and space-based system was built to emulate an actual mission environment. This would require building a hybrid network consisting of a T1 link to the Internet, an 802.11 wireless link between the emulated space experiment and its satellite link, a satellite-to-satellite link, and a firewall gateway at the NASA Tracking and Data Relay Satellite System (TDRSS) ground station in White Sands, New Mexico.

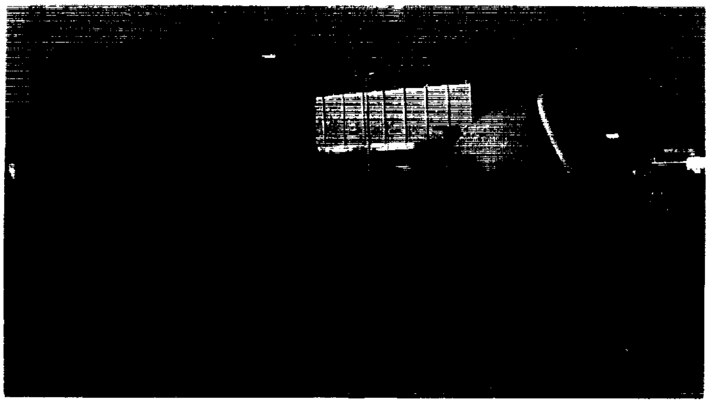

Figure 1.—Tracking and Data Relay Satellite System Internet Link Terminal.

To emulate a ground-to-space network, the NASA TDRSS was chosen because it is the primary satellite system that provides NASA data communications for NASA missions. Modifications were made to the NASA White Sands TDRSS ground station to provide an Internet gateway to NASA TDRSS. The emulated space-based side of the network used the portable S-Band satellite terminal, developed at the NASA Goddard Space Flight Center, known as TILT (TDRSS Internet Link Terminal) which is shown in figure 1. TILT was installed at the Johnson Space Center demonstration site to emulate a satellite link onboard the International Space Station. The NASA White Sands TDRSS ground station has been modified to accept the TILT interface. The TILT interface at White Sands receives the $<10^{-7}$ BER link signal from TDRSS. The TILT remote ground station uses COTS (common off the shelf) equipment including COTS routers and INTELSAT-specified satellite modems. The link was capable of providing 1.0 MBPS throughput. This was more than enough bandwidth to effectively conduct this demonstration.

The TILT satellite terminal had to be set up in a parking lot 300 feet from the demonstration area. To connect the demonstration area's network to the satellite link, an 802.11 wireless bridge was used to provide an 11-MBPS wireless link. Yagi directional antennas were used to provide a solid signal between the TILT 802.11 bridge and the demonstration area 802.11 bridge. Future network topologies aboard the International Space Station may include wireless technologies similar to the ones used in this demonstration.

The extended wireless network interfaced with the demonstration area's 10BaseT network, which emulated the payload network aboard the space station. The payload used for this demonstration was the Mars Surface and Atmosphere Experiment (see fig. 2). This experiment was developed by the NASA Glenn Flight Software Engineering Branch to demonstrate how EWT can lower mission costs and simplify operations by using standards-based protocols to command and control the future experiments.

Figure 2.—Mars Surface and Atmosphere Experiment.

This experiment was interfaced to a modified EPCU (Electronic Power Control Unit) which is the same unit used to control experiments onboard the Space Shuttle and International Space Station. The EPCU was modified with an RS–232 interface and then connected to a server to give it web accessibility. Authorized Internet users were able to actively control the vacuum pumps, view the recorded atmospheric data, and view the experiment through a webcam interface.

One of the main goals of this demonstration was to show how Internet users could access their space-based experiments from their standard Internet connection. An independent network with several workstations was set up in the demonstration area. A local ISP provided a T1 for the Internet connection which enabled users on this network to surf the Internet with a web browser and make a connection with the experiment on the emulated space-based network. This network also was used to launch hacker attacks by security professionals attempting to expose weaknesses in the security architecture. Several attempts that were made by security professionals invited to hack into the network proved to be harmless. Since this experiment was made available to users on the Internet, it did not take long for the hacker community to also accept the challenge. The following section will describe the security architecture that protected the space-based network from unauthorized Internet users. A diagram of the network is displayed in figure 3.

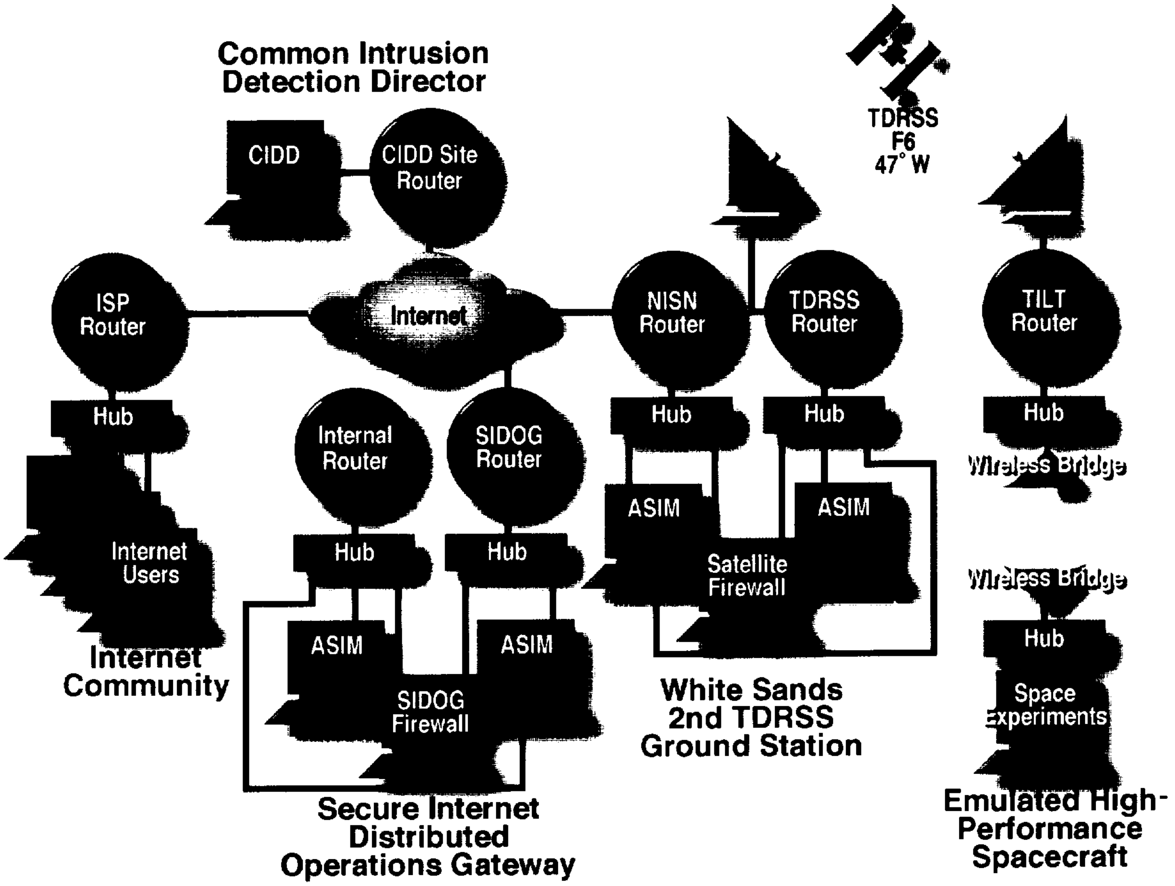

Figure 3.—Security architecture that protected the space-based network.

Veridian Information Solutions (VIS) engineers provided the networking security for the demonstration. The heart and soul of the security system is a combination of VPN (Virtual Private Network) gateways, SIDOG™ (Secure Internet Distributed Operations Gateway), CIDD™ (Common Intrusion Detection Director), and assorted ASIM™ (Automated Security Incident Measurement) workstations.

The SIDOG defines all mission parameters. It is the gateway to the space network. All traffic destined for the satellite uplink passes through the SIDOG gateway. Mission planner's coordinate with the SIDOG operator's to define who has access, what they have access to and when they have access. All of these parameters are configured into the SIDOG management system.

ASIM workstations located at the SIDOG and the TDRSS ground station provide the intrusion detection security for the network. The ASIM workstations monitor every single packet data on both sides of the firewall, inside and outside of the trusted network. Any packets that do not meet the stringent security parameters are rejected and reported to the CIDD. When security parameters change, the CIDD will push new parameters to the ASIM workstations to keep them updated with the latest security configurations.

The CIDD serves as the watchman. It monitors all security incidents reported by the firewall systems located at the SIDOG and the TDRSS ground station. The CIDD will report and automatically shut down any suspicious activity detected by any of the ASIM monitors. Operators at the CIDD console would then take the necessary action to report the suspicious activity to the appropriate authorities. The SIDOG and CIDD can be located anywhere in the world but for the demonstration held at Inspection 2000, the SIDOG was located at the Veridian facility in San Antonio, Texas, and the CIDD was located in the demonstration area at the Lyndon B. Johnson Space Center. By locating the CIDD at the demonstration site, people attending the demonstration were able to watch in real time how the CIDD logged and rejected the various hacking attempts that occurred during the presentation.

VPN technology provides the encrypted tunnels between the researcher and the space experiment. For a typical session between a researcher and a space experiment, four VPN tunnels would be built across the Internet. A diagram of these tunnels is displayed in figure 4.

In the demonstration at Inspection 2000, when the researcher needed to access the experiment he/she would establish the first VPN tunnel (1) (VPN–1) with the SIDOG. An added measure of security was installed in this demonstration by using a biometric mouse that recorded the researcher's fingerprint. Not only did the researcher have to use an ID and password, but his/her fingerprint had to match the fingerprint file located at the SIDOG.

After the user was authenticated at the SIDOG, a second VPN tunnel (2) (VPN–2) was built between the SIDOG and the Satellite Firewall located at the TDRSS ground station in White Sands, New Mexico. The VPN Gateway at the TDRSS ground station decrypts the packets and then forwards them to the TDRSS uplink.

Two more VPN tunnels are built during this session to provide an added layer of security. These tunnels (3 and 4) (VPN–3 and VPN–4) are built between the CIDD and the ASIM workstations at the SIDOG and the Satellite Firewall. All suspicious traffic detected by the ASIM workstations is reported to the CIDD via a VPN tunnel. At this point the CIDD uses the VPN tunnels to communicate to the appropriate firewall to terminate the perpetrator.

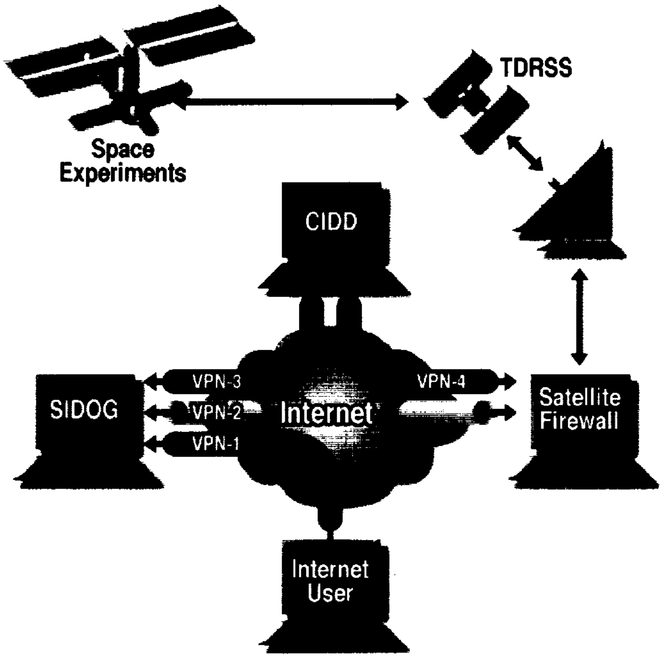

Figure 4.—Visual Private Network tunnels.

During a demonstration, there were several security incidents reported from Internet connections from New York to Japan. In each case, the CIDD terminated all of the suspicious connections before they were able to gain access.

The demonstration proved that by using COTS networking products and applying EWT to space-based assets, NASA's mission operations could be simplified which would result in significant cost savings. The demonstration also proved that by deploying a multilayered security architecture like the one displayed at Inspection 2000, secure Internet command and control of space assets is possible and is a viable architecture for future NASA missions.

NASA Space Communications Program: http://spacecom.grc.nasa.gov/
NASA EWT: http://vic.lerc.nasa.gov/techxfer/anatomy.html
Veridian Space Services: http://www.veridian.com/domains/space.asp
TDRSS Information: http://nmsp.gsfc.nasa.gov/tdrss/
TILT Satellite Terminal: http://nmsp.gsfc.nasa.gov/pet/tilt.htm

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2001	**3. REPORT TYPE AND DATES COVERED** Technical Memorandum

4. TITLE AND SUBTITLE

Space Internet-Embedded Web Technologies Demonstration

5. FUNDING NUMBERS

WU–322–20–2A–00

6. AUTHOR(S)

David A. Foltz

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
John H. Glenn Research Center at Lewis Field
Cleveland, Ohio 44135–3191

8. PERFORMING ORGANIZATION REPORT NUMBER

E–12997

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Washington, DC 20546–0001

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

NASA TM—2001-211145

11. SUPPLEMENTARY NOTES

Responsible person, David A. Foltz, organization code 5610, 216–433–5077.

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified - Unlimited
Subject Categories: 60, 61, and 62 Distribution: Nonstandard

Available electronically at http://gltrs.grc.nasa.gov/GLTRS
This publication is available from the NASA Center for AeroSpace Information, 301–621–0390.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 words)***

The NASA Glenn Research Center recently demonstrated the ability to securely command and control space-based assets by using the Internet and standard Internet Protocols (IP). This is a significant accomplishment because future NASA missions will benefit by using Internet standards-based protocols. The benefits include reduced mission costs and increased mission efficiency. The Internet-Based Space Command and Control System Architecture demonstrated at the NASA Inspection 2000 event proved that this communications architecture is viable for future NASA missions.

14. SUBJECT TERMS

Internet; Computer information security; Satellite communication

15. NUMBER OF PAGES

11

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	